Федеральное государственное бюджетное образовательное учреждение
инклюзивного высшего образования
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-
ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет Прикладной математики и информатики
Кафедра Информационных технологий и прикладной математики

Проректор по УМР
_____ Ковалева М.А.
«31» августа 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

образовательная программа специальности
45.05.01 «Перевод и переводоведение»
Блок Б1.Б.09 «Дисциплины (модули)», базовая часть

Квалификация (степень) выпускника
специалитет

Специализация
Лингвистическое обеспечение международных отношений

Форма обучения
очная

Курс 5 семестр 9

Москва
2020

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего профессионального образования направления специальности 45.05.01 «Перевод и переводоведение» (уровень специалитета), утвержденного Приказом Министерства образования и науки Российской Федерации от 17 октября 2016 № 1290 "Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 45.05.01 «Перевод и переводоведение» (уровень специалитета). Зарегистрировано в Минюсте России 03 ноября 2016 г. Регистрационный № 44245

Составители рабочей программы: МГГЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность

_____ Белоглазов А.А. «20» августа 2020 г.
подпись Ф.И.О. Дата

Рецензент: МГГЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность

_____ Никольский А.Е. «21» августа 2020 г.
подпись Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Информационных технологий и прикладной математики (протокол № 1 от «24» августа 2020 г.)

Зав. кафедрой ИТиПМ _____ Петрунина Е.В. «24» августа 2020 г.
подпись Ф.И.О. Дата

СОГЛАСОВАНО
Начальник
Учебного отдела
«28» августа 2020 г. _____ И.Г. Дмитриева
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО
Декан
факультета
«28» августа 2020 г. _____ _____
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО
Заведующий
библиотекой
«28» августа 2020 г. _____ В.А. Ахтырская
(дата) (подпись) (Ф.И.О.)

ОДОБРЕНО
УЧЕБНО-МЕТОДИЧЕСКИМ
СОВЕТОМ МГГЭУ
№ 1 от 31 августа 20

1. Цели и задачи дисциплины, ее место в учебном процессе, требования к уровню освоения содержания дисциплины

1.1. Цели и задачи изучения дисциплины.

Целью изучения дисциплины является подготовка студентов к освоению организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, ознакомление с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение способов применения методов защиты информации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

Задачи:

- раскрытие специфики защиты компьютерных сетей как объекта научного исследования;
- определение основных этапов и базовых концептуальных подходов к созданию систем защиты компьютерных сетей в рамках исторического развития отечественной и зарубежной науки;
- знакомство со способами и особенностями создания систем защиты компьютерных сетей на различных уровнях взаимодействия с окружением;
- приобретение студентами навыков аналитического и эмпирического исследования систем компьютерной защиты сетей;
- выработка целостного представления о различных аспектах строения и функционирования систем компьютерной защиты сетей на всех ее уровнях;
- рост навыков в сфере создания систем компьютерной защиты сетей и умения применять полученные знания на практике.

1.2. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

В результате изучения дисциплины студенты должны:

Знать:

- правовые основы защиты компьютерной информации;
- организационные, технические и программные методы защиты информации в АСОИУ;
- стандарты, модели и методы шифрования;
- методы идентификации пользователей;
- методы защиты программ от вирусов и вредоносных программ;
- требования к системам информационной защиты АСОИУ и компьютерных сетей.

Уметь:

- применять методы защиты компьютерных сетей при проектировании АСОИУ в различных предметных областях.

Владеть:

- способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий;
- способностью решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности.

Изучение данной дисциплины направлено на формирование следующих компетенций:

Код компетенции	Наименование результата обучения
ОПК-1	способностью работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять её в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке;
ОПК-5	способностью самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных;
ПК-8	способностью применять методику ориентированного поиска информации в справочной, специальной литературе и компьютерных сетях.

1.3. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности в профессиональной деятельности» относится к базовой части блока Б1. «Дисциплины (модули)» и изучается в 9-м семестре.

Изучение дисциплины «Основы информационной безопасности в профессиональной деятельности» основывается на знаниях, полученных при прохождении дисциплины «Интернет-ресурсы».

Изучение дисциплины «Основы информационной безопасности в профессиональной деятельности» формирует знание и навыки в области информационных технологиях, что развивает способность работать с различными источниками информации, информационными ресурсами и технологиями, а также применять переводческие трансформации.

2. Содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Семестр-9, вид отчетности: экзамен.

№ раздела	Наименование раздела, тема	Содержание раздела	Форма текущего контроля
1.	**Основные понятия информационной безопасности и защиты информации.**	Анализ угроз информационной безопасности. Анализ угроз корпоративных сетей. Характерные особенности сетевых атак. Угрозы и уязвимости беспроводных сетей. Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы. Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем. Меры и средства обеспечения информационной безопасности. Пути решения проблем информационной безопасности.	Устный опрос, проверка практических работ
2.	**Стандарты информационной безопасности.**	Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты ISO/IEC 17799:2002 (BS 7799:2000).	Устный опрос, проверка практических

		Германский стандарт BSI. Международный стандарт ISO 15408. «Общие критерии безопасности информационных технологий». Стандарты для беспроводных сетей. Стандарты информационной безопасности для Интернета. Отечественные стандарты безопасности информационных технологий. Стандарт «Критерии оценки безопасности информацион0ных технологий» ГОСТ Р ИСО/МЭК 15408.	работ
3.	**Криптографическая защита информации.**	Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Алгоритмы шифрования DES и 3-DES. Стандарт шифрования ГОСТ 28147-89. Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования. Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA. Функции хэширования. Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.	Устный опрос, проверка практических работ
4.	**Раздел 4 Принципы многоуровневой защиты корпоративной информации.**	Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений. Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений.	Устный опрос, проверка практических работ
5.	**Защита информации в компьютерных сетях, антивирусная защита.**	Концепция построения виртуальных защищенных сетей VPN. PN-решения для построения защищенных сетей. Современные VPN-продукты.	Устный опрос, проверка практических работ
6.	**Защита удаленного доступа.**	Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей. Централизованный контроль удаленного доступа. Протокол Kerberos.	Устный опрос, тестирование

3. Структура дисциплины

Вид работы	Трудоемкость, часов	
	9 семестр	**Всего**
Общая трудоемкость	**108**	**108**
Аудиторная работа:	**48**	**48**
Лекции (Л)	16	16
Практические занятия (ПЗ)	24	24
Лабораторные работы (ЛР)	8	8
Зачет (З)		
Самостоятельная работа:	**24**	**24**
Курсовой проект (КП), курсовая работа (КР)		
Расчетно-графическое задание (РГЗ)	12	12
Реферат (Р)		
Самостоятельное изучение разделов	12	12
Контрольная работа (К)		
Самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)		
Подготовка к экзамену	**36**	**36**
Вид итогового контроля (указать вид контроля)	**Экзамен**	**Экзамен**

4. Распределение видов учебной работы и их трудоемкости по разделам

Разделы дисциплины, изучаемые в 9 семестре:

№ раз-дела	Наименование разделов	Количество часов				
		Всего	Аудиторная Работа			Внеауд. работа СР
			Л	ПЗ	ЛР	
1.	Основные понятия информационной безопасности и защиты информации	10	2	4	-	4
2.	Стандарты информационной безопасности	10	2	2	2	4
3.	Криптографическая защита информации	12	2	4	2	4
4.	Принципы многоуровневой защиты корпоративной информации	14	4	4	2	4
5.	Защита информации в компьютерных сетях, антивирусная защита	18	4	6	2	4
6.	Защита удаленного доступа	10	2	4	-	4
	Экзамен	36				
	Итого:	**108**	**16**	**24**	**8**	**24**

5. Тематический план учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа студентов, курсовая работа (проект)	Объем часов/ зачетных единиц	Образовательные технологии	Формируемые компетенции/ уровень освоения*	Формы текущего контроля
1	2	3	4	5	6
		108/3			
1. Основные понятия информационной безопасности и защиты информации	**Лекции**	2	Вводная лекция, Информационная лекция, Обзорная лекция	ОПК-1/1 ОПК-5/1 ПК-8/1	Устный опрос
	1. Анализ угроз информационной безопасности.				
	2. Характерные особенности сетевых атак.				
	3. Угрозы и уязвимости беспроводных сетей.				
	4. Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы.				
	5. Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем.				
	6. Меры и средства обеспечения информационной безопасности.				
	7. Пути решения проблем информационной безопасности.				
	Практические занятия	4	Практикум на ЭВМ.	ПК-8/2,3	Проверка практических работ
	1. Анализ угроз информационной безопасности.				
	2. Характерные особенности сетевых атак.				
	3. Угрозы и уязвимости беспроводных сетей.				
	4. Тенденции развития ИТ-угроз. Криминализация атак на компьютерные сети и системы.				
	5. Появление кибероружия для ведения технологических кибервойн. Обеспечение информационной безопасности компьютерных систем.				
	6. Меры и средства обеспечения информационной безопасности.				
	Пути решения проблем информационной безопасности.				
	Самостоятельная работа студента	4	Саморазвивающее обучение	ПК-8/2,3	Устный опрос
	1. Меры и средства обеспечения информационной безопасности.				

	2	Пути решения проблем информационной безопасности.				
2. Стандарты информационной безопасности	**Лекции**		2	Информационная лекция,	ОПК-1/1 ОПК-5/1 ПК-8/1	Устный опрос
	1.	Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты ISO/IEC 17799:2002 (BS 7799:2000).				
	Практические занятия		2	Практикум на ЭВМ.	ПК-8/2,3	Проверка практических и лабораторных работ
	1.	Германский стандарт BSI. Международный стандарт ISO 15408. «Общие критерии безопасности информационных технологий». Стандарты для беспроводных сетей. Стандарты информационной безопасности для Интернета.				
	Лабораторная работа		2	IT-технологии		
	1.	Стандарты ISO/IEC 17799:2002 (BS 7799:2000).				
	Самостоятельная работа студента		4	Саморазвивающее обучение	ПК-8/2,3	Устный опрос
	1.	Самостоятельное изучение разделов				
3. Криптографическая защита информации	**Лекции**		2	Проблемная лекция, лекция-беседа, лекция-визуализация	ОПК-1/1 ОПК-5/1 ПК-8/1	Устный опрос
	1.	Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Алгоритмы шифрования DES и 3-DES. Стандарт шифрования ГОСТ 28147-89.				
	2.	Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования.				
	3.	Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA.				
	4.	Функции хэширования.				
	5.	Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.				
	Практические занятия		4	Практикум на	ПК-8/2,3	Проверка

	1.	Стандарт шифрования AES. Другие симметричные криптоалгоритмы. Основные режимы работы блочного симметричного алгоритма. Особенности применения алгоритмов симметричного шифрования.		ЭВМ.		практических и лабораторных работ
	2.	Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA.				
	3.	Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.				
	Лабораторная работа		2	IT-технологии	ПК-8/2,3	
	1.	Шифрование и расшифровка текста различными алгоритмами				
	Самостоятельная работа студента		4	Саморазвивающее обучение	ПК-8/2,3	Устный опрос
	1	Электронная цифровая подпись. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2001.				
4. Принципы многоуровневой защиты корпоративной информации	**Лекции**		4	Информационная лекция	ОПК-1/1 ОПК-5/1 ПК-8/1	Устный опрос
	1.	Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений.				
	2.	Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений				
	Практические занятия		4	Ролевое построение семинара - докладчик и оппоненты	ПК-8/2,3	Проверка практических и лабораторных работ
	1.	Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений.				
	2.	Многоуровневый подход к обеспечению информационной безопасности КИС. Безопасность «облачных» вычислений				
	Лабораторная работа		2	IT-технологии		
	1.	Облачные технологии защиты информации				
	Самостоятельная работа студента		4	Саморазвивающее обучение	ПК-8/2,3	Устный опрос
	1.	Корпоративная информационная система с традиционной структурой. Системы «облачных» вычислений.				

5. Защита информации в компьютерных сетях, антивирусная защита защиты корпоративной информации	**Лекции**		4	Проблемная лекция, лекция-беседа, лекция-визуализация	ОПК-1/1 ОПК-5/1 ПК-8/1	Устный опрос
	1.	Защита информации в компьютерных сетях				
	2	Антивирусная защита.				
	Практические занятия		6	Ролевое построение семинара - докладчик и оппоненты	ПК-8/2,3	Проверка практических и лабораторных работ
	1.	Защита информации в компьютерных сетях				
	2.	Антивирусная защита.				
	Лабораторная работа		2	IT-технологии		
	1.	Виды компьютерных вирусов и защита от них				
	1.	**Самостоятельная работа студента** Самостоятельное изучение разделов	4	Саморазвивающее обучение	ПК-8/2,3	Устный опрос
6. Защита удаленного доступа	**Лекции**		2	Проблемная лекция, лекция-беседа, лекция-визуализация	ОПК-1/1 ОПК-5/1 ПК-8/1	Устный опрос
	1.	Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей.				
	2.	Централизованный контроль удаленного доступа. Протокол Kerberos**.**				
	Практические занятия		4	Ролевое построение семинара - докладчик и оппоненты	ПК-8/2,3	Проверка практических работ
	1	Особенности удаленного доступа. Средства и протоколы аутентификации удаленных пользователей.				
	2.	Централизованный контроль удаленного доступа. Протокол Kerberos**.**				
	1.	**Самостоятельная работа студента** Самостоятельное изучение разделов	4	Саморазвивающее обучение	ПК-8/2,3	Устный опрос
	Экзамен		36			
	Итого		108/3			

***** В таблице уровень усвоения учебного материала обозначен цифрами:

1. – репродуктивный (освоение знаний, выполнение деятельности по образцу, инструкции или под руководством);
2. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач; применение умений в новых условиях);
3. – творческий (самостоятельное проектирование экспериментальной деятельности; оценка и самооценка инновационной деятельности).

6. Образовательные технологии

6.1.Интерактивные образовательные технологии, используемые в аудиторных занятиях

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
9	Л	Проблемная лекция, лекция-беседа, лекция-визуализация	10
	ПР	Ролевое построение семинара - докладчик и оппоненты.	14
	ЛР	IT-технологии	6
Итого:			30

6.2 Особенности обучения лиц с ОВЗ и инвалидностью

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом индивидуальных психофизических особенностей, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Для получения обучающимися, имеющими ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: обучающийся должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии.

Для обучения и контроля обучающихся с нарушениями координации движений предусмотрено проведение тестирования с использованием компьютера.

Во время аудиторных занятий обязательно использование средств обеспечения наглядности учебного материала с помощью мультимедийного проектора. Скорость изложения материала должна учитывать ограниченные физические возможности студентов.

7. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

7.1.Организация входного, текущего и промежуточного контроля обучения

- Текущий контроль – опрос, устный опрос, тестирование, контрольная работа.
- Промежуточная аттестация – экзамен.

7.2. Организация контроля (пример)

Пример опроса по дисциплине:

1. Каковы назначение и особенности функционирования
2. протокола SET.
3. Каковы назначение и функциональность протоколов SSL и IPSec.
4. Каково назначение стандарта ГОСТ Р ИСО/МЭК 15408. Назовите и охарактеризуйте три основные части этого стандарта.
5. Обобщенная схема криптосистемы шифрования
6. Классификация криптографических алгоритмов
7. Схема симметричной криптосистемы шифрования
8. Алгоритм шифрования DES и 3DES
9. Стандарт шифрования ГОСТ 28147-89
10. Стандарт шифрования AES
11. Режимы работы блочного симметричного алгоритма

12. Дайте определение однонаправленной функции. Каковы особенности однонаправленных функции.

13. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.

14. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш-функция?

15. Дать определение понятия «идентификация», «аутентификация», «авторизация», «администрирование».

16. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?

17. Опишите метод аутентификации на основе мно при0зовых паролей. Каковы его недостатки?

18. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?

19. Сформулируйте принцип строгой аутентификации.

20. Объясните назначение PIN-кода и особенности его использования.

21. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используют для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?

22. Опишите функциональность и характеристики смарт-карт и USB-токенов.

23. Опишите методы биометрической аутентификации пользователя.

24. Объясните принцип управления доступом по схеме однократного входа с авторизацией SSO.

7.3. Тематика рефератов, проектов, творческих заданий, эссе и т.п. – нет.

7.4. Курсовая работа - не предусмотрена

7.5. Вопросы к экзамену

1. Уточнение задач информационной безопасности организации. Изучение источников, рисков и форм атак на информацию в АСОИУ.
2. Изучение источников, рисков и форм атак на информацию в АСОИУ. Классификация рисков и основные задачи обеспечения безопасности информации в АСОИУ.
3. Изучение Российского законодательства по защите информационных технологий. Изучение нормативно-правовой информации, определяющей функционирование систем защиты. Разработка политики информационной безопасности организации.
4. Изучение международных и Государственных стандартов информационной безопасности.
5. Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ.
6. Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем.
7. Изучение принципов идентификации и механизмов подтверждения подлинности пользователя. Правила формирования электронной цифровой подписи.
8. Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.
9. Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия. Изучение методов борьбы с компьютерными

вирусами и средств защиты информации в Internet. Угрозы исходящие от использования «электронной почты».

10. Изучение требований по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению АСОИ. Порядок и правила организации аудита информационной безопасности АСОИУ и предприятия в целом.
11. Понятие информационной безопасности. Характеристики информации с позиции безопасности.
12. Классификация угроз безопасности информации.
13. Классификация угроз безопасности распределенных вычислительных систем
14. Модель OSI.
15. Объясните понятие «политика безопасности организации».
16. Какие разделы должна содержать документально оформленная политика безопасности?
17. Какие проблемы решает верхний уровень политики безопасности?
18. Какие задачи решает средний уровень политики безопасности?
19. Каковы особенности нижнего уровня политики безопасности?
20. Сформулируйте главную задачу стандартов информационной безопасности с позиций производителей и потребителей продуктов информационных технологий, а также специалистов по сертификации этих продуктов.
21. Назовите основные международные стандарты информационной безопасности.
22. Дайте краткую характеристику международного стандарта 17799 (BS 7799).
23. Каковы основные особенности германского стандарта BSI «Руководство по защите информационных технологий для базового уровня защищенности».
24. Перечислите стандарты для беспроводных сетей и дайте их краткую характеристику.
25. Назовите стандарты информационной безопасности для Internet.

7.6 Критерии оценки

- оценка **«отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, причем не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач;
- оценка **«хорошо»** выставляется студенту, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;
- оценка «**удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;
- оценка **«неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

8. Сведения о материально-техническом обеспечении дисциплины

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет

9. Учебно-методическое обеспечение дисциплины

9.1. Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1009606 . Режим доступа: по подписке.
2. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2018. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа: https://new.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/925825. Режим доступа: по подписке.
3. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1094244. Режим доступа: по подписке.

9.2. Дополнительная литература

1. Каймин, В. А. Информатика: Учебник / Каймин В. А. - 6-е изд. - Москва : НИЦ ИНФРА-М, 2016. - 285 с.:- (Высшее образование: Бакалавриат). - ISBN 978-5-16-003778-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/542614 . Режим доступа: по подписке.
2. Исаев, Г. Н. Управление качеством информационных систем: Учебное пособие / Исаев Г.Н. - Москва :НИЦ ИНФРА-М, 2016. - 248 с. (Высшее образование: Бакалавриат) ISBN 978-5-16-011794-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/543677. Режим доступа: по подписке.

9.3. Учебно-методическое и информационное обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы)

1. http://asu.gubkin.ru/ - Методы и средства защиты информации;
2. http://www.osp.ru/ - Журнал «Открытые Системы»;
3. http://www.compulog.ru/ - Журнал «HackZone»;
4. http://www.iso.org/ Международные стандарты безопасности ISO;
5. http://www.citforum.ru/ - CITforum;
6. http://www.groteck.ru/security_ru - Журнал «Информационная безопасность»;
7. http://securitylab.ru/ - портал SecurityLab;
8. http://www.networkdoc.ru/ - NetworkdocRu;
9. http://cryptography.ru/- Математическая криптография.
10. Электронная библиотека «Знаниум»: режим доступа: https://znanium.com//

11. Электронная библиотека «Юрайт»: https://urait.ru

9.4. Программное обеспечение

1. Сетевой компьютерный класс, оснащенный современной техникой.
2. Офисный программный пакет (например, свободно-распространяемый Open Office).
3. Web-браузер Mozilla Firefox или Google Chrome.
4. Экран для проектора.